Discrete Mathematics

The Integers and Division, Modular Arithmetic

Abdul Hameed

http://informationtechnology.pk/pucit

abdul.hameed@pucit.edu.pk

The Integers and Division

- The part of mathematics involving the integers and their properties belongs to the branch of mathematics called number theory
- Basic concepts of number theory used throughout computer science.
- Divisibility and Modular Arithmetic

The Integers and Division

- **Of course, you already know what the integers are, and what division is…**
- **However: There are some specific notations, terminology, and theorems associated with these concepts which you may not know.**
- **These form the basics of *number theory*.**
  - **Vital in many important algorithms today (hash functions, cryptography, digital signatures; in general, on-line security).**

The divides operator

- **New notation: 3 | 12**
  - **To specify when an integer evenly divides another integer**
  - **Read as "3 divides 12"**
- **The not-divides operator: 5 ∤ 12**
  - **To specify when an integer does *not* evenly divide another integer**
  - **Read as "5 does not divide 12"**

Divides, Factor, Multiple

- Let $a,b \in \mathbf{Z}$ with $a \neq 0$.

- **Defn.:** $a|b \equiv$ "*a divides b*" $:\equiv (\exists\, c \in \mathbf{Z}: b=ac)$
- **"There is an integer *c* such that *c* times *a* equals *b*."**
  - Example: $3|{-12} \Leftrightarrow$ **True**, but $3|7 \Leftrightarrow$ **False**.

- **Iff *a* divides *b*, then we say *a* is a *factor* or a *divisor* of *b*, and *b* is a *multiple* of *a*.**

- Ex.: "*b* is even" $:\equiv 2|b$. Is 0 even? Is −4?

Results on the divides operator

- If a | b and a | c, then a | (b+c)
  - Example: if 5 | 25 and 5 | 30, then 5 | (25+30)
- If a | b, then a | bc for all integers c
  - Example: if 5 | 25, then 5 | 25*c for all ints c
- If a | b and b | c, then a | c
  - Example: if 5 | 25 and 25 | 100, then 5 | 100

("common facts" but good to repeat for background)

Divides Relation

- **Theorem:** $\forall a,b,c \in \mathbf{Z}$:
  1. $a|0$
  2. $(a|b \wedge a|c) \rightarrow a \mid (b + c)$
  3. $a|b \rightarrow a|bc$
  4. $(a|b \wedge b|c) \rightarrow a|c$

Corollary: If a, b, c are integers, such that a | b and a | c, then a | mb + nc whenever m and n are integers.

Proof of (2)

- Show $\forall a,b,c \in Z: (a|b \wedge a|c) \rightarrow a \mid (b + c)$.
- Let a, b, c be any integers such that $a|b$ and $a|c$, and show that $a \mid (b + c)$.
- By defn. of $|$, we know $\exists s: b=as$, and $\exists t: c=at$.
- Let s, t, be such integers.
- Then $b+c = as + at = a(s+t)$.
- So, $\exists u: b+c=au$, namely $u=s+t$. Thus $a|(b+c)$.

Divides Relation

Corollary: If a, b, c are integers, such that a | b and a | c, then a | mb + nc whenever m and n are integers.

Proof:

From previous theorem part 3 (i.e., $a|b \rightarrow a|be$) it follows that a | mb and a | nc ; again, from previous theorem part 2 (i.e., $(a|b \wedge a|c) \rightarrow a \mid (b + c)$) it follows that a | mb + nc

The Division "Algorithm"

- **Theorem:**
- **Division Algorithm --- Let a be an integer and d a positive**
- **integer. Then there are *unique* integers q and r, with $0 \leq r < d$,**
- **such that $a = dq + r$.**

It's really a theorem, not an algorithm…

Only called an "algorithm" for historical reasons.

- *q* is called the **quotient**
- *r* is called the **remainder**
- *d* is called the **divisor**
- *a* is called the **dividend**

- *q* is called the **quotient**
- *r* is called the **remainder**
- *d* is called the **divisor**
- *a* is called the **dividend**

- **What are the quotient and remainder when 101 is divided by 11?**

a d q r

$101 = 11 \times 9 + 2$

We write:

q = 9 = 101 div 11

r = 2 = 101 mod 11

- If $a = 7$ and $d = 3$, then $q = 2$ and $r = 1$, since $7 = (2)(3) + 1$.
- If $a = -7$ and $d = 3$, then $q = -3$ and $r = 2$, since $-7 = (-3)(3) + 2$.

So: given positive **a** and (positive) **d**, in order to get **r** we repeatedly subtract **d** from **a**, as many times as needed so that what remains, **r**, is less than **d**.

Given negative **a** and (positive) **d**, in order to get **r** we repeatedly add **d** to **a**, as many times as needed so that what remains, **r**, is positive (or zero) and less than **d**.

Theorem:

Division "Algorithm" --- Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

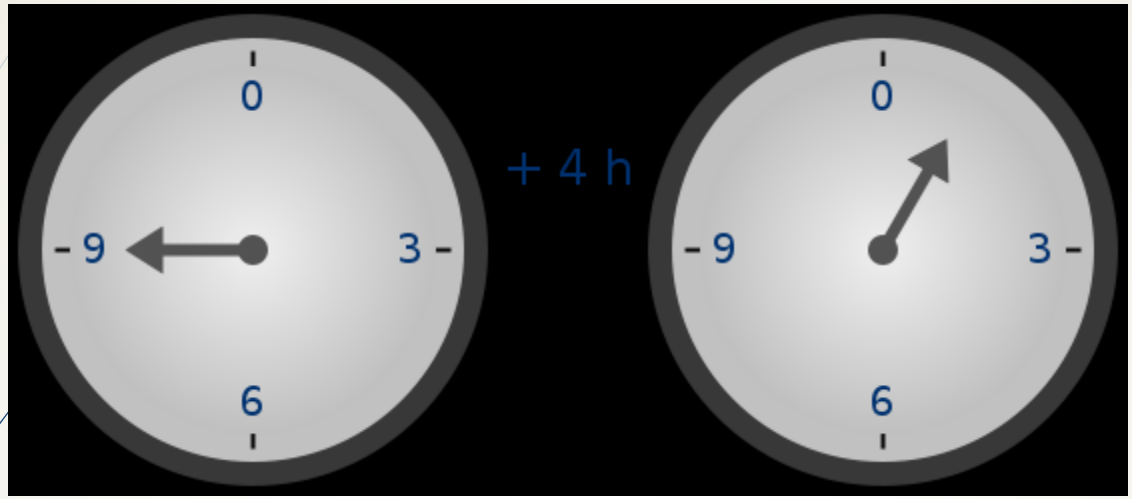
Modular arithmetic

- **If *a* and *b* are integers and *m* is a positive integer, then**
- **"*a* is *congruent to b modulo m*" if *m* divides *a-b***
  - **Notation: $a \equiv b \pmod{m}$**
  - **Rephrased: $m \mid a-b$**
  - **Rephrased: $a \bmod m = b \bmod m$**
  - **If they are not congruent: $a \equiv b \pmod{m}$**

Note "≠" sign.

- Example: Is 17 congruent to 5 modulo 6?
  - Rephrased: $17 \equiv 5 \pmod{6}$
  - As 6 divides 17-5, they are congruent
- Example: Is 24 congruent to 14 modulo 6?
  - Rephrased: $24 \equiv 14 \pmod{6}$
  - As 6 does not divide 24-14 = 10, they are not congruent

Note: this is a different use of "≡" than the meaning "is defined as" used before.



Time-keeping on a clock gives an example of modular arithmetic. (mod 12 in the US; or mod 24, using the 24hr clock. Naturally imposed by the periodicity of earth's rotation.)

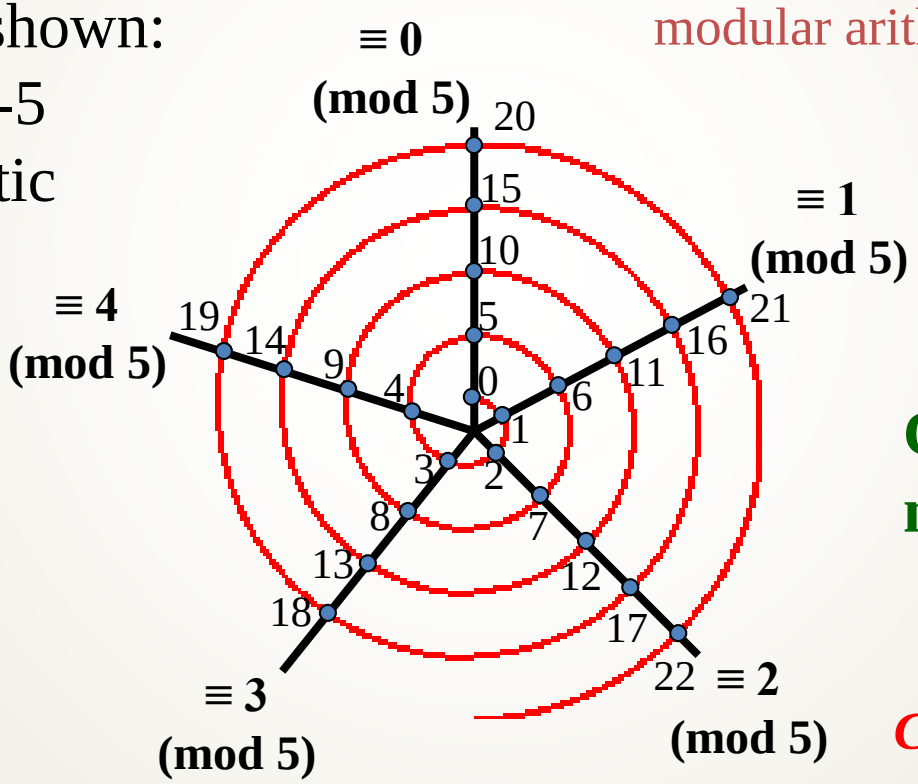
Where is -1?

Spiral Visualization of mod

Where is -7?

The spiral/circular view is useful to keep in mind when doing modular arithmetic!

Example shown: modulo-5 arithmetic



Congruence classes modulo 5.

Collapses infinite set of numbers into 5 classes.

So, e.g., 19 is congruent to 9 modulo 5.

More on congruences

- **Theorem: Let *a* and *b* be integers, and let *m* be a positive integer.**
- **Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$**

Theorem:

Let *m* be a positive integer. The integers *a* and *b* are congruent modulo *m* if and only if there is an integer *k* such that $a = b + km$

Example: 17 and 5 are congruent modulo 6, so

$17 = 5 + 2*6$

$5 = 17 - 2*6$

Even even more on congruence

- **Theorem: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$,**
- **then $a+c \equiv (b+d) \pmod{m}$ and $ac \equiv bd \pmod{m}$**

- Example
  - We know that $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$
  - Thus, $7+11 \equiv (2+1) \pmod{5}$, or $18 \equiv 3 \pmod{5}$
  - Thus, $7*11 \equiv 2*1 \pmod{5}$, or $77 \equiv 2 \pmod{5}$

Applications of Congruences

- Hashing functions
  - $h(k) = k \bmod m$
- Pseudorandom numbers
  - $x_{n+1}=(ax_n+c) \bmod m$
- Cryptology
  - Caesar cipher: $f(p) = (p+k) \bmod 26$